METHOD FOR ESTABLISHING A COMMON KEY FOR A GROUP OF AT LEAST THREE SUBSCRIBERS

(2) What is claimed is:

1. A method for establishing a common key for a group of at least three subscribers, using a publicly known mathematical group G and a publicly known element of the group $g \in G$ of large order,

wherein

a) each subscriber (Ti) generates a message ($Ni = g^{zi} \bmod p$) from the publicly known element (g) of the group (G) and a random number (zi) selected or generated by him/her and sends it to all other subscribers (Tj),

b) each subscriber (Ti) generates a transmission key (k^{ij}) from the messages (Nj) received from the other subscribers (Tj, $j \neq i$) and his/her random number (zi) according to the function $k^{ij} := Nj^{zi} = (g^{zj})^{zi}$, the key being also known to subscriber (Tj) due to the equation $k^{ij} = k^{ji}$,

c) each subscriber (Ti) sends his/her random number (zi) to all other subscribers (Tj) in encrypted form by generating the message (Mij) according to $Mij := E(k^{ij}, zi)$, with $E(k^{ij}, zi)$ being a symmetrical encryption algorithm in which the data record (zi) is encrypted with the common transmission key (k^{ij}), and

d) the common key (k) to be established is determined by each subscriber (Ti) from his/her own random number (zi) and the random numbers (zj), $j \neq i$, received from the other subscribers according to the equation

$$k := f(z1, ..., zn),$$

it being required for f to be a symmetrical function which is invariant under the permutation of its arguments.